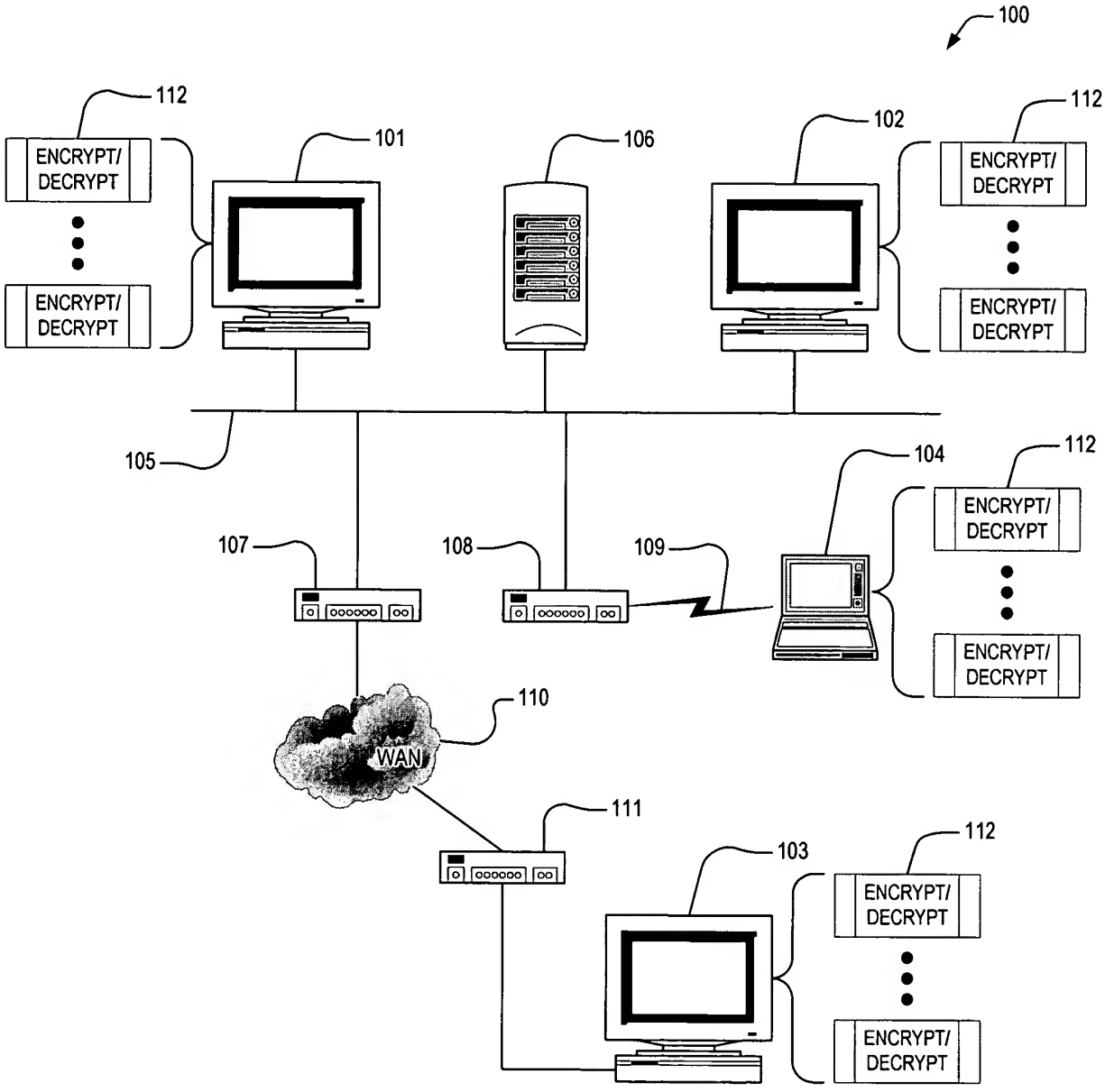
100
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
101
106
102
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
105
104
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
107
108
109
110
WAN
111
103
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT

FIG. 1

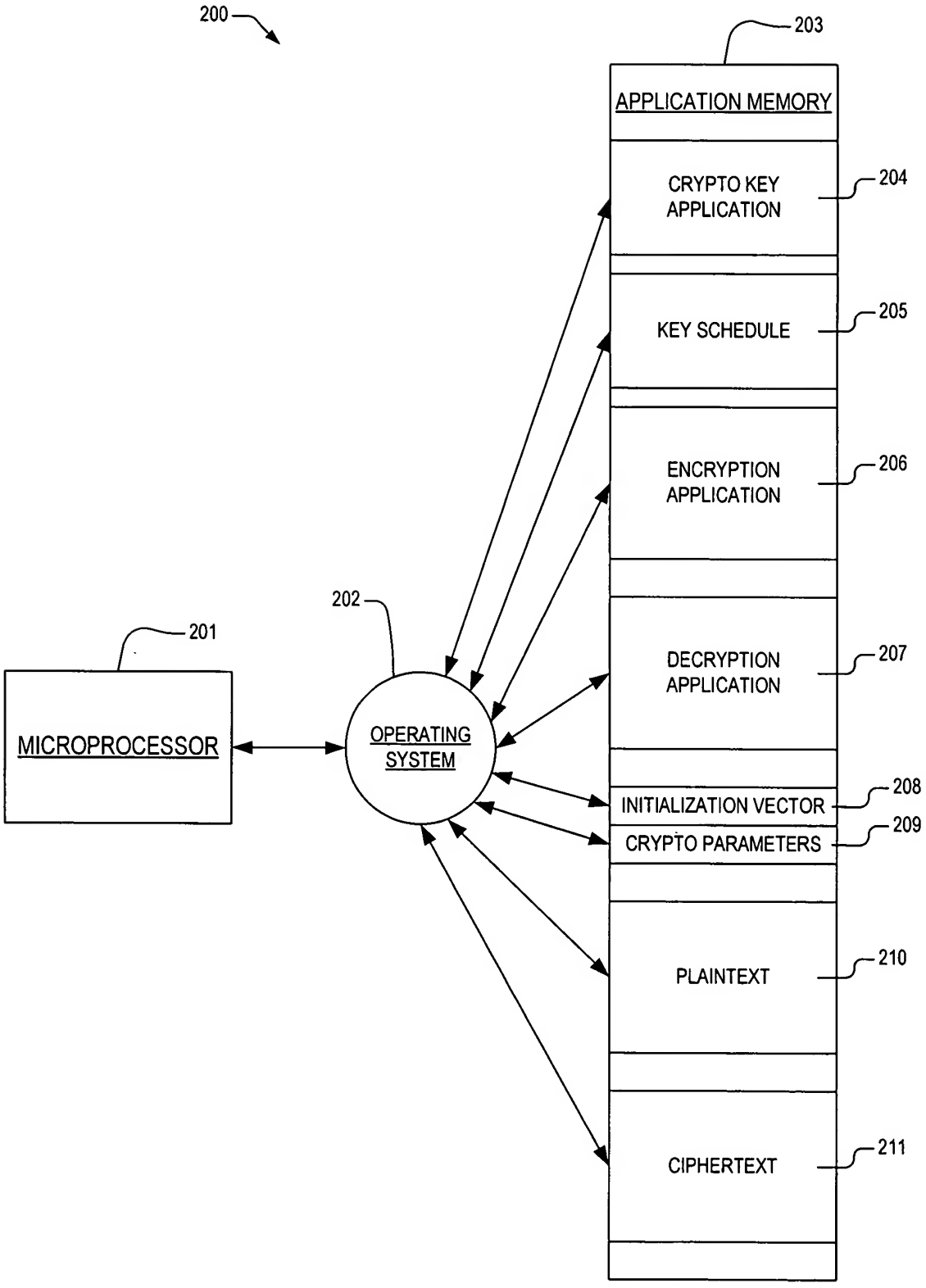
200
203
APPLICATION MEMORY
CRYPTO KEY APPLICATION
204
KEY SCHEDULE
205
ENCRYPTION APPLICATION
206
DECRYPTION APPLICATION
207
202
201
MICROPROCESSOR
OPERATING SYSTEM
INITIALIZATION VECTOR
208
CRYPTO PARAMETERS
209
PLAINTEXT
210
CIPHERTEXT
211

FIG. 2

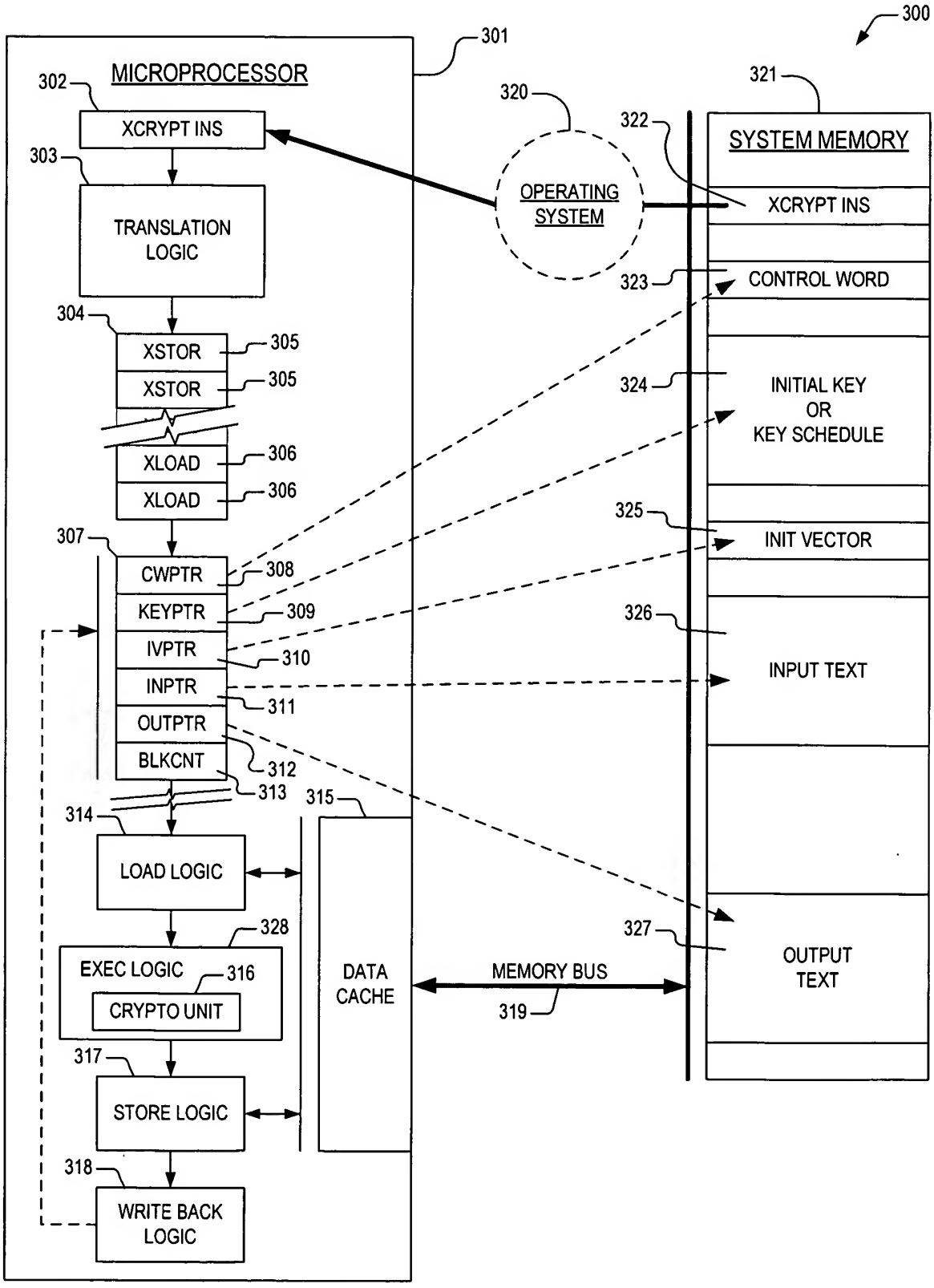
300
301
MICROPROCESSOR
302
XCRYPT INS
303
TRANSLATION LOGIC
304
XSTOR
305
XSTOR
305
XLOAD
306
XLOAD
306
307
CWPTR
308
KEYPTR
309
IVPTR
310
INPTR
311
OUTPTR
312
BLKCNT
313
314
LOAD LOGIC
328
EXEC LOGIC
316
CRYPTO UNIT
317
STORE LOGIC
318
WRITE BACK LOGIC
315
DATA CACHE
320
OPERATING SYSTEM
321
SYSTEM MEMORY
322
XCRYPT INS
323
CONTROL WORD
324
INITIAL KEY OR KEY SCHEDULE
325
INIT VECTOR
326
INPUT TEXT
327
OUTPUT TEXT
MEMORY BUS
319

FIG. 3

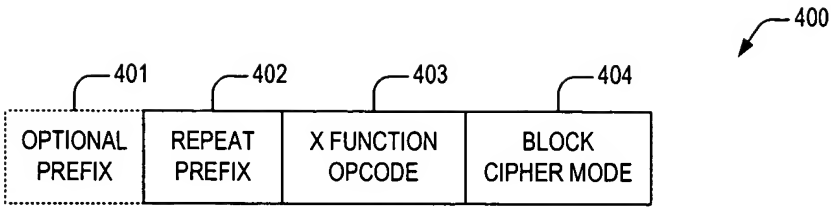

FIG. 4

500

BCM VALUE	MODE
0xC8	ELECTRONIC CODE BOOK (ECB)
0xD0	CIPHER BLOCK CHAINING (CBC)
0xE0	CIPHER FEEDBACK (CFB)
0xE8	OUTPUT FEEDBACK (OFB)
ALL OTHER VALUES	RESERVED

FIG. 5

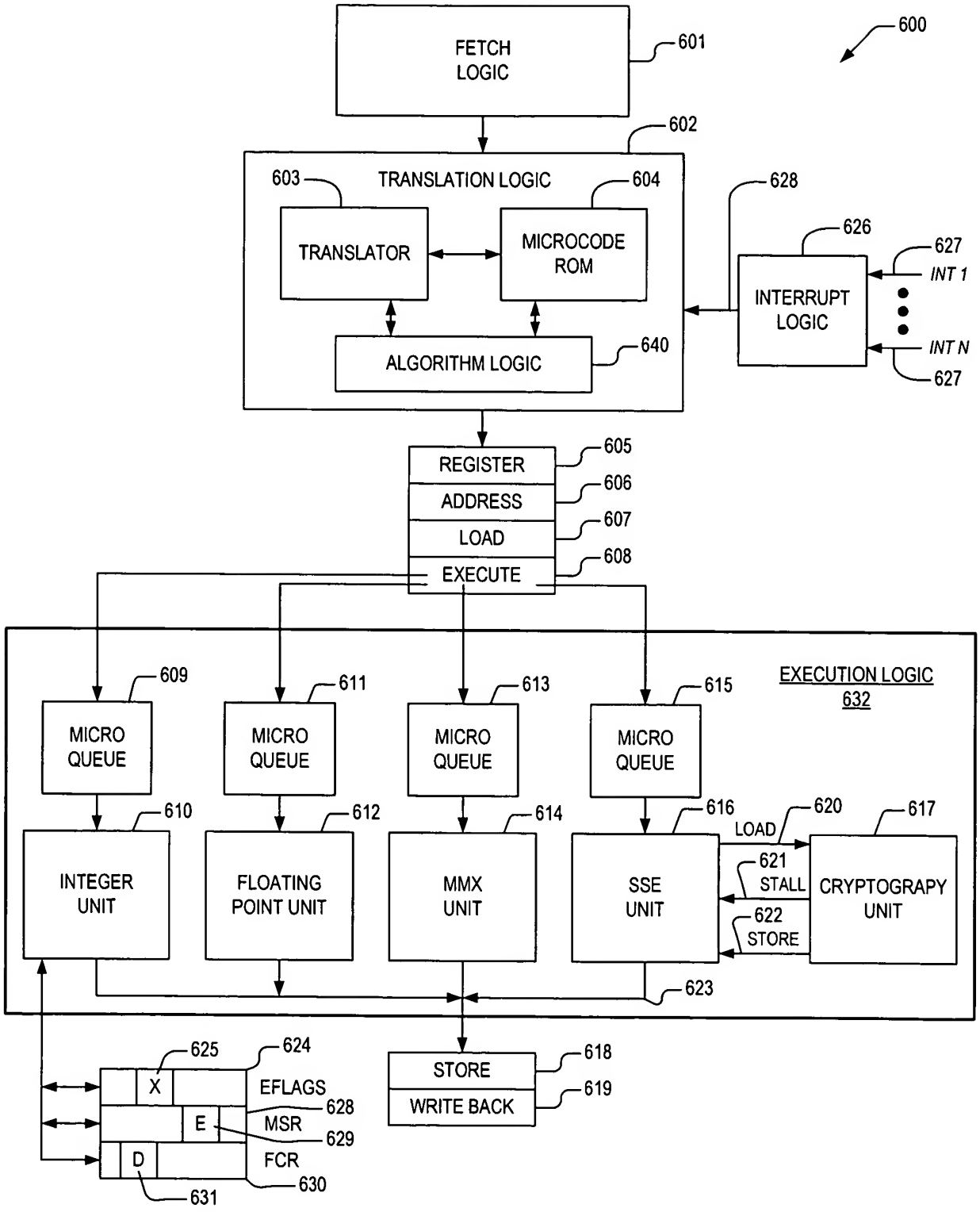
FETCH LOGIC
601
600
602
603
TRANSLATION LOGIC
604
628
626
627
INT 1
TRANSLATOR
MICROCODE ROM
INTERRUPT LOGIC
INT N
627
ALGORITHM LOGIC
640
REGISTER
605
ADDRESS
606
LOAD
607
EXECUTE
608
EXECUTION LOGIC 632
609
611
613
615
MICRO QUEUE
MICRO QUEUE
MICRO QUEUE
MICRO QUEUE
610
612
614
616
620
617
LOAD
INTEGER UNIT
FLOATING POINT UNIT
MMX UNIT
SSE UNIT
621
STALL
CRYPTOGRAPY UNIT
622
STORE
623
625
624
X
EFLAGS
628
E
MSR
629
D
FCR
630
631
STORE
618
WRITE BACK
619

FIG. 6

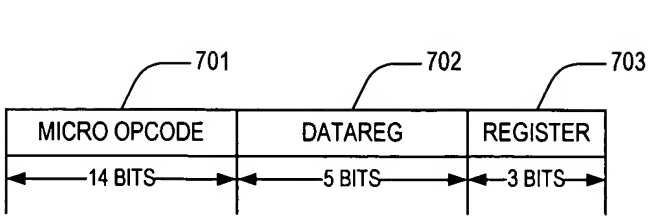

FIG. 7

800

VALUE	OPERATION
000	RESERVED
001	RESERVED
010	LOAD CONTROL WORD (CW) REGISTER
011	RESERVED
100	LOAD INPUT-0 (IN-0) REGISTER AND START CRYPTOGRAPHY UNIT
101	LOAD INPUT-1 (IN-1) REGISTER
110	LOAD CRYPTO KEY-0 REGISTER (LOWER 128 BITS OF KEY)
111	LOAD CRYPTO KEY-1 REGISTER (UPPER 128 BITS OF KEY)

FIG. 8

900

VALUE	OPERATION
000	RESERVED
001	RESERVED
010	RESERVED
011	RESERVED
100	STORE OUTPUT-0 (OUT-0) REGISTER
101	STORE OUTPUT-1 (OUT-1) REGISTER
110	RESERVED
111	RESERVED

FIG. 9

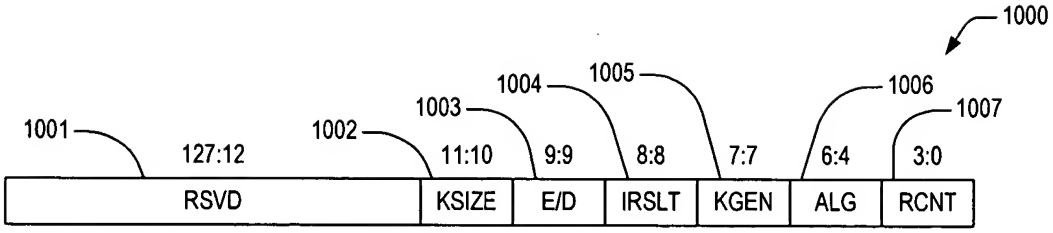
1000
1001
127:12
1002
11:10
1003
9:9
1004
8:8
1005
7:7
1006
6:4
1007
3:0
RSVD
KSIZE
E/D
IRSLT
KGEN
ALG
RCNT

FIG. 10

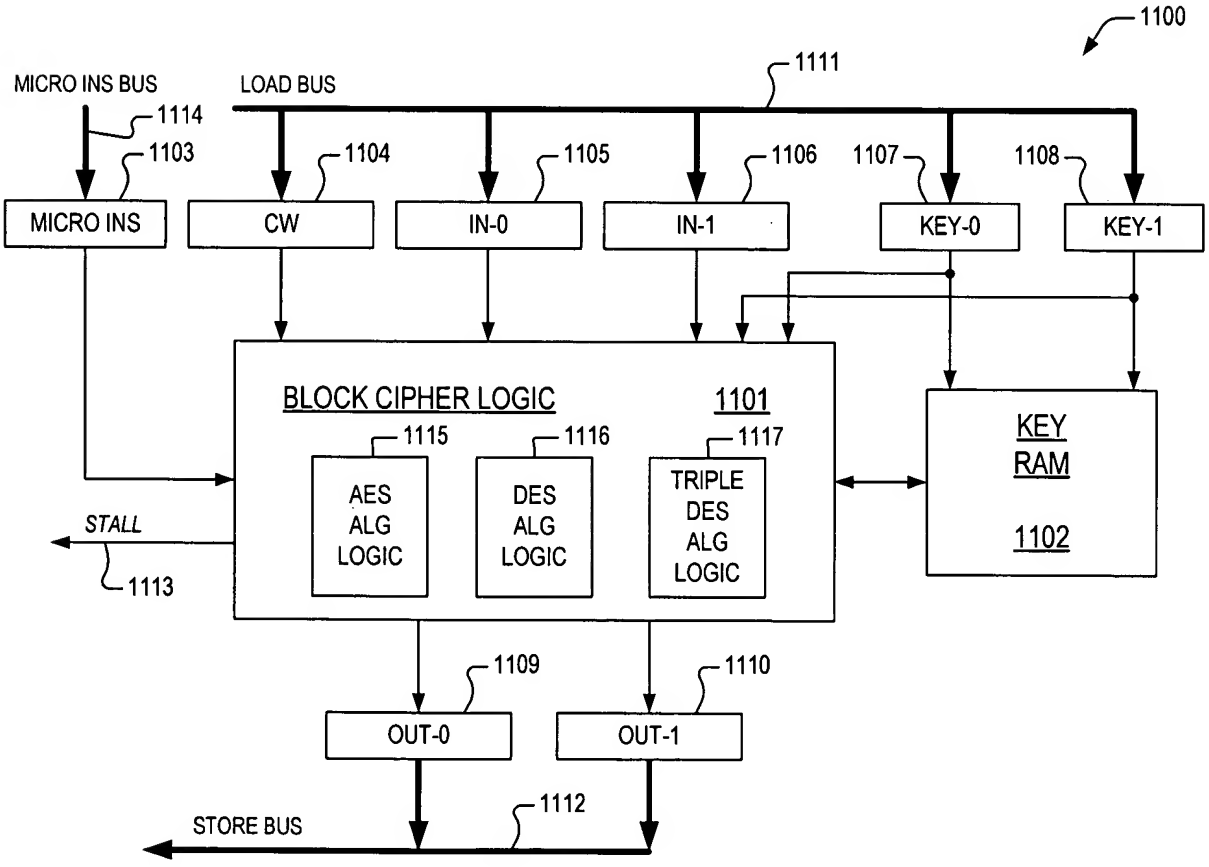
1100
1111
MICRO INS BUS
LOAD BUS
1114
1103
1104
1105
1106
1107
1108
MICRO INS
CW
IN-0
IN-1
KEY-0
KEY-1
BLOCK CIPHER LOGIC
1101
1115
1116
1117
AES ALG LOGIC
DES ALG LOGIC
TRIPLE DES ALG LOGIC
KEY RAM
1102
STALL
1113
1109
1110
OUT-0
OUT-1
1112
STORE BUS

FIG. 11

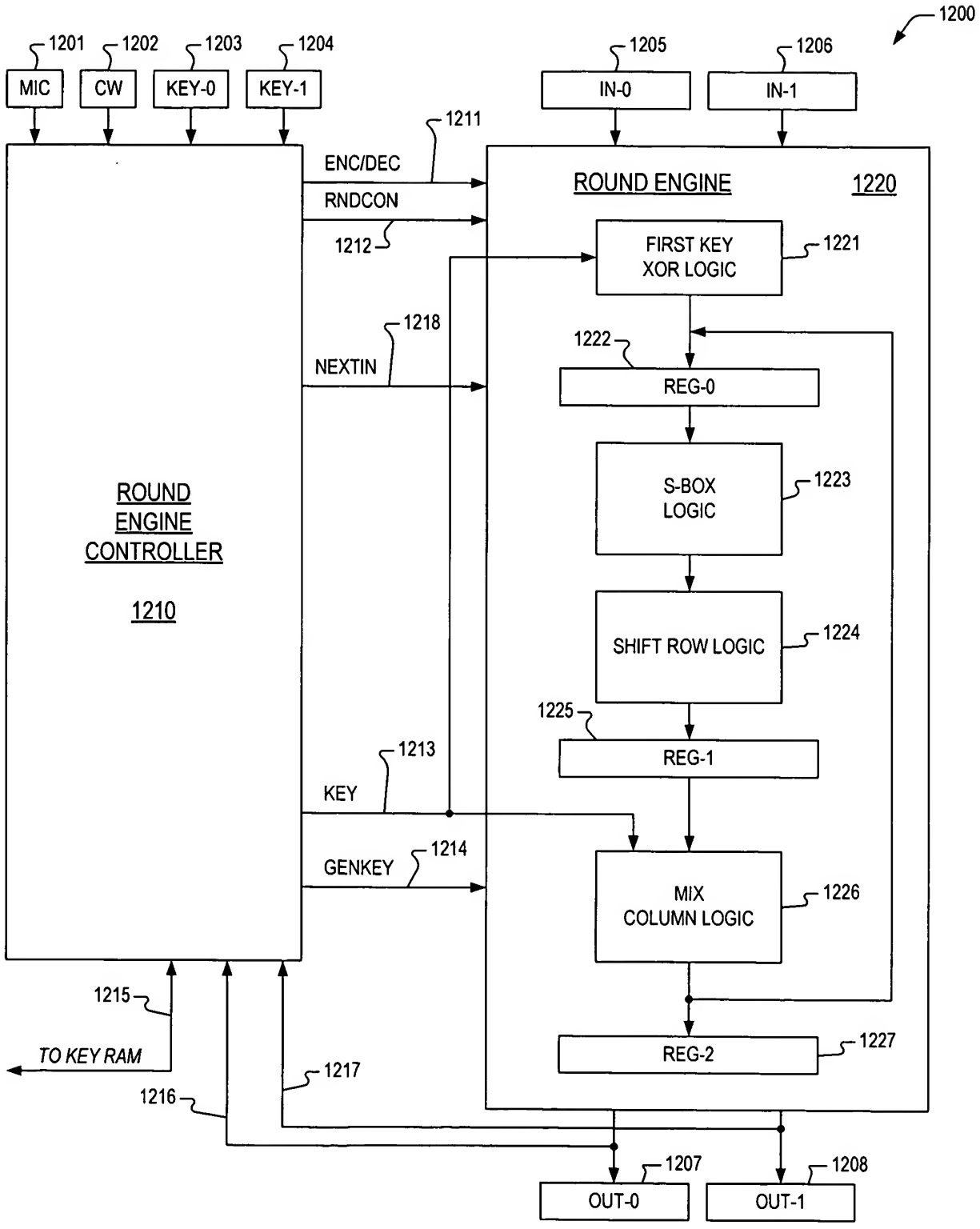
1200
1201
MIC
1202
CW
1203
KEY-0
1204
KEY-1
1205
IN-0
1206
IN-1
1211
ENC/DEC
RNDCON
1212
ROUND ENGINE
1220
FIRST KEY XOR LOGIC
1221
1218
NEXTIN
1222
REG-0
S-BOX LOGIC
1223
ROUND ENGINE CONTROLLER
1210
SHIFT ROW LOGIC
1224
1225
REG-1
1213
KEY
1214
GENKEY
MIX COLUMN LOGIC
1226
1215
TO KEY RAM
REG-2
1227
1217
1216
1207
1208
OUT-0
OUT-1

FIG. 12

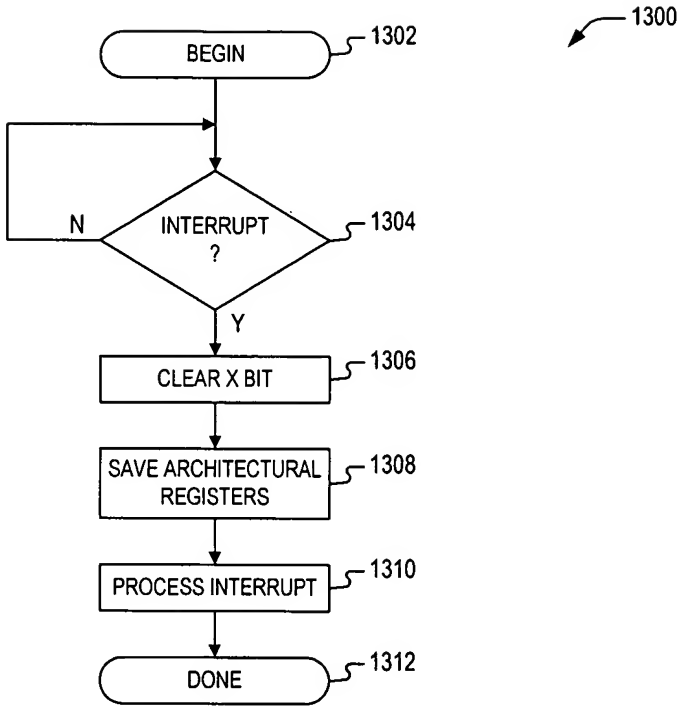
1300
BEGIN
1302
INTERRUPT ?
1304
N
Y
CLEAR X BIT
1306
SAVE ARCHITECTURAL REGISTERS
1308
PROCESS INTERRUPT
1310
DONE
1312

FIG. 13

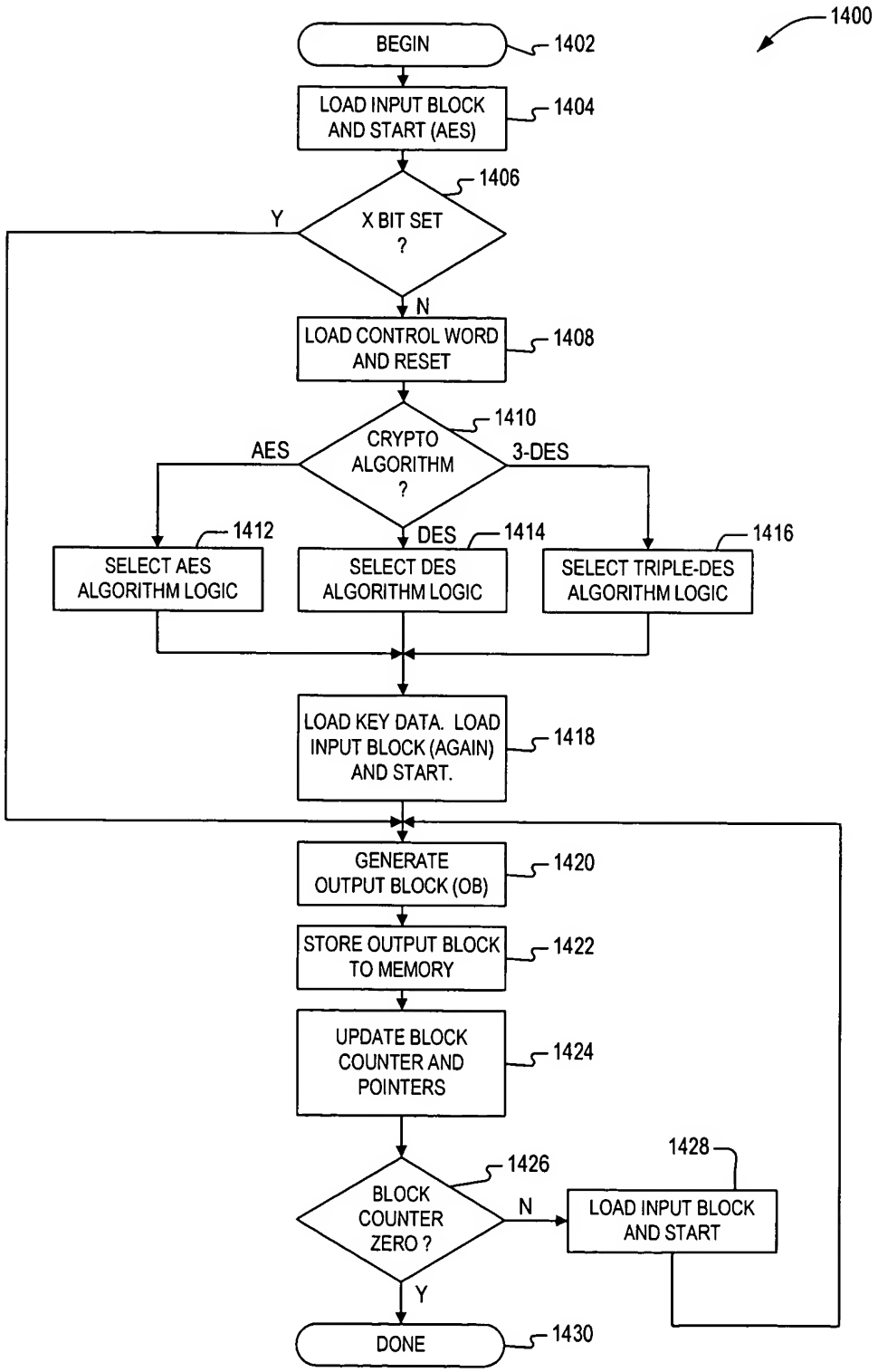
1400
BEGIN
1402
LOAD INPUT BLOCK AND START (AES)
1404
1406
X BIT SET ?
Y
N
LOAD CONTROL WORD AND RESET
1408
1410
CRYPTO ALGORITHM ?
AES
3-DES
DES
1412
SELECT AES ALGORITHM LOGIC
1414
SELECT DES ALGORITHM LOGIC
1416
SELECT TRIPLE-DES ALGORITHM LOGIC
LOAD KEY DATA. LOAD INPUT BLOCK (AGAIN) AND START.
1418
GENERATE OUTPUT BLOCK (OB)
1420
STORE OUTPUT BLOCK TO MEMORY
1422
UPDATE BLOCK COUNTER AND POINTERS
1424
1426
BLOCK COUNTER ZERO ?
N
1428
LOAD INPUT BLOCK AND START
Y
DONE
1430

FIG. 14